



DigitalGate PRAポートフォワード 管理者マニュアル

2009年09月01日 Version 1.1

bit-drive

***DigitalGate PRA* ポートフォワード管理者マニュアル目次**

- [1] PRAポートフォワード機能概要
- [2] 事前検討項目
- [3] PRAポートフォワード機能を使用する
- [4] 利用者への導入
- [5] PRAポートフォワードクライアント セットアップにあたって
- [6] PRAポート転送ルール設定例

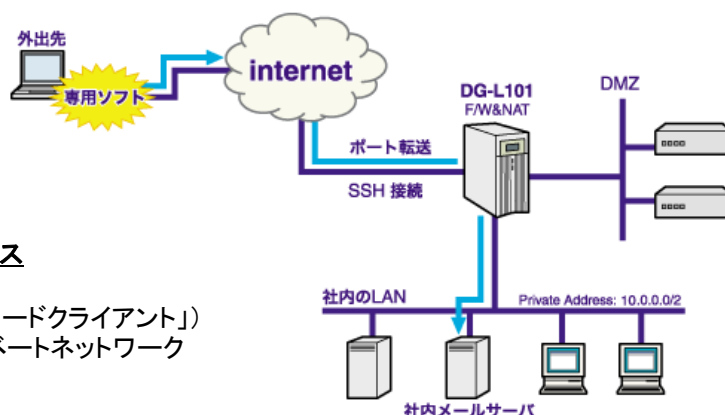
[1] PRAポートフォワード機能概要

■「PRAポートフォワード機能」とは?

PRAポートフォワードは、外部ネットワークから社内リソース(メールサーバー、Webサーバーなど)へ安全にアクセスするための機能です。

ポートフォワード(ポート転送)機能により、外部ネットワークから社内リソースにアクセス

専用クライアントソフト(以下、「ポートフォワードクライアント」)からアクセスすれば、DigitalGateがプライベートネットワークへリクエストを転送してくれます。



OpenSSHを利用して、セキュリティを確保

DigitalGateとポートフォワードクライアントでは、OpenSSHのポート転送機能をベースにして、PRAポートフォワード機能を実現しています。

OpenSSHは強力な暗号化機能と認証機能を備えており、クライアントPCとDigitalGateの間でセキュアな通信路を確保し、悪意のある第三者によるなりすましも防ぐことができます。

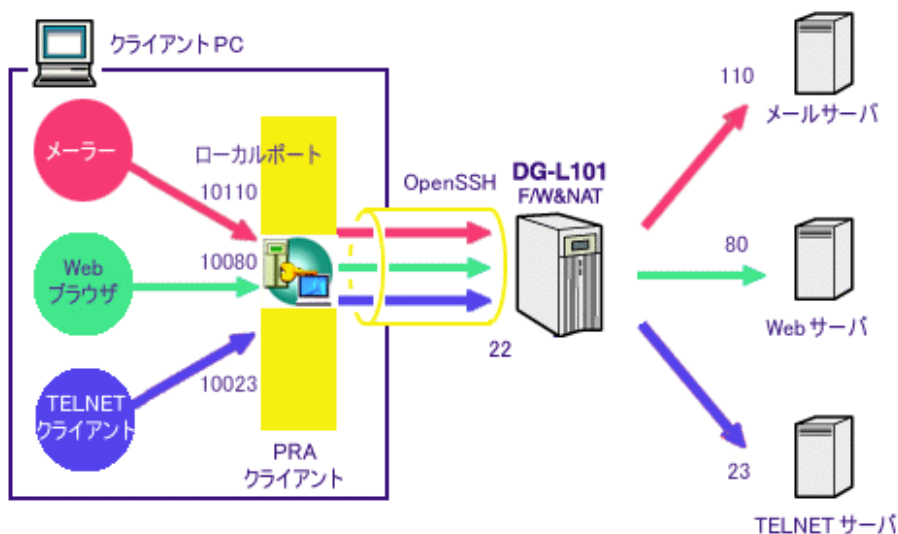
複数の社内リソースにアクセス可能

DigitalGateは、接続しているクライアントPCのポート(以下「ローカルポート」)によって、転送先を選択することができます。これによって、複数の社内リソースを社外から同時に利用することができます。

■「PRAポートフォワード機能」の仕組み

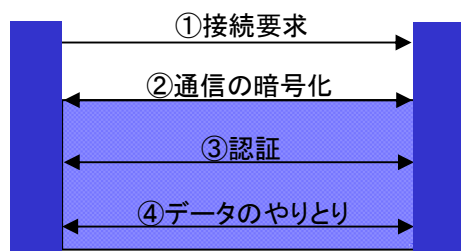
PRAポートフォワード機能は、以下のような仕組みで社内リソースへのアクセスを実現しています。

- まず、ポートフォワードクライアントは、DigitalGateとの間にOpenSSHで接続します。
- メールやウェブブラウザなどのアプリケーションは、社内のサーバーではなく、ポートフォワードクライアントにアクセスします。
- ポートフォワードクライアントは、それらの通信をひきうけます。そして、OpenSSHによって暗号化された経路を使って、DigitalGateに転送します。
- DigitalGateはローカルポート毎に指定されたサーバにそれぞれの通信をさらに転送します。



■OpenSSHのセキュリティ

OpenSSHは図に示すような仕組みで安全な通信を実現しています。



クライアントからサーバーに対して接続要求がだされる(①)と、まず通信を暗号化するためのやり取りが行われます(②)。このやり取りが成功すれば、その後の通信は全て暗号化されます。その上でサーバーがクライアントを認証し(③)、成功すれば、データのやり取りができるようになります(④)。

■OpenSSHによる暗号化の仕組み

OpenSSHのデータ暗号化には共通鍵暗号系を使います。暗号化アルゴリズムは、PRAポートフォワードでは3DESを利用しています。暗号化に使う共通鍵を公開鍵暗号方式によって安全に交換します。その手順は以下のとおりです。

- | | | |
|----------|--------|---------------------------------------|
| サーバー側: | ホスト鍵 | ... 公開鍵暗号方式の鍵の対。 |
| | サーバー鍵 | ... 公開鍵暗号方式の鍵の対(一時間毎に再作成します)。 |
| クライアント側: | セッション鍵 | ... 実際の暗号化に使う共通鍵暗号方式の鍵(接続する度に再作成します)。 |

1. サーバーはクライアントにホスト公開鍵とサーバー公開鍵を送ります。
2. クライアントはセッション鍵を生成します。セッション鍵は256bitのランダムな文字列です。
3. クライアントはセッション鍵をホスト公開鍵とサーバー公開鍵で二重で暗号化し、サーバーに送り返します。
4. サーバーは送り返されたセッション鍵をホスト秘密鍵とサーバー秘密鍵で復号化します。
5. サーバーは、確認のため、セッション鍵で暗号化されたメッセージをクライアントに送ります。
6. クライアントがメッセージを確認できれば、成功、できなければ失敗となります。

■RSA認証のしくみ

PRAポートフォワードは、ユーザーの認証にRSA認証を利用しています。RSA認証は、公開鍵暗号方式のデファクトスタンダードといえる方式で、全世界で広く利用されています。

RSA認証の手順は以下のとおりです。

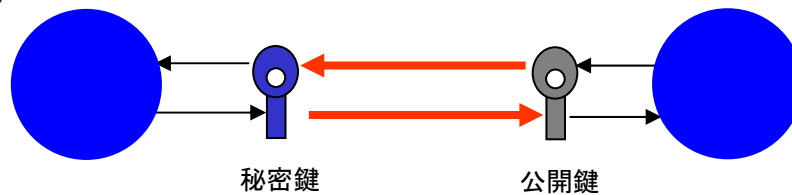
1. サーバーは、256bitランダムな文字列 (challenge) を生成します。
2. サーバーは、認証するユーザーの公開鍵でchallengeを暗号化してクライアントに送ります。
3. クライアントは、サーバーから送られてきたchallengeを、自分の秘密鍵で復号化します。
4. クライアントは、復号化されたchallengeのMD5のhash値をサーバーに送り返します。
5. サーバーは、送り返されてきたchallengeのMD5のhash値と、サーバーで保持していたchallengeのMD5のhash値を比べて、等しければ認証に成功、そうでなければ失敗となります。

■公開鍵暗号方式とは？

公開鍵暗号方式とは、「公開鍵」と「秘密鍵」という一対の鍵の組を使ってデータの暗号化・復号化を行う方式です。

秘密鍵によって暗号化されたデータは対になる公開鍵でのみ復号化され、公開鍵によって暗号化されたデータは対になる秘密鍵でのみ復号化されます。また、公開鍵からその対になる秘密鍵を類推することは非常に困難です。

PRAポートフォワードでは、DigitalGateが公開鍵を、専用クライアントソフトが秘密鍵を保持しています。第三者に秘密鍵が漏洩すると、簡単に自分になりすまされてしまうので、秘密鍵の管理は厳重に行う必要があります。PRAポートフォワードをインストールしたPCを紛失した場合には、DigitalGate設定画面から公開鍵（ユーザー鍵）の再作成を行ってください。



[2] 事前検討項目

■外部からアクセスさせるプライベートネットワーク内のリソースを決める

まず、PRAポートフォワード機能を利用して外部ネットワークからアクセスを許可するリソースを**契約者のセキュリティポリシーなどを考慮して**決めてください。

例) アクセスを許可するリソース		
サーバー名	IPアドレス	サービスのポート
■メールサーバー	10.0.0.2	110(POP3)、25(SMTP)
■社内Webサーバー	10.0.0.3	80(HTTP)
■社内スケジュール用Webサーバー	10.0.0.4	8080

※一つのサーバー内で複数のサービスを許可する場合は、1サービスを1リソースと考えてください。

例) メールサーバー(POP3,SMTP) → 2リソース

次に、各リソースを下記の表にあてはめ、クライアントPCが利用するローカルポートを決めてください。

転送先IPアドレス (サーバーのIPアドレス)	転送先ポート番号 (サーバーのポート番号)	ローカルポート番号	コメント
10.0.0.2	110	10110	POPサーバ

重複不可

利用者に
わかり易い
コメントを

※ローカルポートには、クライアントPCで既に使用されているポートは指定できません。

例) ウィルス駆除ソフトで110番が使用されいてる → POPサーバーは10110に

設定例は [6] PRAポート転送ルール設定例 を参照

■外部からアクセスさせる利用者を決める

次に、DigitalGateにアカウントを持つユーザーの中から、PRAポートフォワード許可するユーザーを**セキュリティポリシーにしたがって**決めてください。

RSAによる認証とは言え利用者に依存するセキュリティとなるため、慎重に利用者を決定してください。なお、利用者には使用上の注意を説明し、十分に理解させてください。

接続を許可するユーザー	接続を禁止するユーザー
例) tanaka,yamada	例) watanabe

[3] PRAポートフォワード機能を使用する

PRAポートフォワード機能を使用する場合、PRAポートフォワードの設定で、「接続が許可されているユーザー」を設定し、ポート転送ルールを設定します。

[2] で検討した結果を元に、下記の設定を行なってください。

■「接続が許可されているユーザー」を設定する

1. 管理画面から [システムオプション]—[PRA]—[PRAポートフォワード] を選びます。



2. [接続が禁止されているユーザー] から、PRAポートフォワード機能を使用させるユーザーを選択し、[許可] をクリックします。(複数ユーザー選択可能)



3. [パスワード] に管理者用のパスワードを入力します。
4. [実行] をクリックします。[許可しました] というメッセージが表示され、設定が変更されます。

「接続が許可されているユーザー」が一人もいないと、
サーバーは「無効」になっています

サーバーを「有効」にするためには
「接続が許可されているユーザー」を設定して下さい。

■「PRA転送ルール」を設定する

1. 管理画面から [システムオプション]－[PRA]－[PRAポートフォワード] を選びます。
2. [ポート転送ルール] の [追加] をクリックします。

3. PRAポートフォワードで利用を許可する社内のリソースを設定します。

転送先IPアドレス	: 外部からアクセスを許可するサーバーのIPアドレス 例) 10.0.0.2
転送先ポート	: 外部からアクセスを許可するサーバー上で利用するサービスのポート番号 例) サービスがPOP3の時、ポート番号は『110』
ローカルポート	: ユーザーのPC上で、利用するサービスと対応付けるポート番号(重複不可) ※既に使用されている番号以外なら何でもOK
コメント	: ユーザーに表示される設定の名前 ユーザー接続時に、各設定の名前として表示されます。 例)『メールサーバー』

3. [パスワード] に管理者用のパスワードを入力します。
4. [実行] をクリックします。[追加しました] というメッセージが表示され、設定が追加されます。

PRAポートフォワードを利用するユーザーが使用出来る社内リソースはこの画面で設定した『PRA転送ルール』にある設定だけです

PRAポートフォワード機能をご利用の際は必ず1つ以上の設定を行なって下さい

[4] 利用者への導入

利用者がセットアップを行うまでに次の3つの作業が発生します。事前に各項目を検討し、利用者への導入方法を決めてください。

1. DigitalGateへのアクセス

利用者が Digital Gate にアクセスする方法は2種類あります。PRAポートフォワード機能は、クライアントソフトを使用した通信は保護致しますが、利用者がソフトウェアを取得するまでの間に第三者の手に渡ると大変危険です。そのため、**安全性の面から、(a)を推奨します。**利用者が (b) の方法でソフトウェアを取得する場合には、危険性を理解した上で行なってください。

(a) HTTPS経由でWAN側IPアドレスへアクセス

HTTPSを使用するため、通信が暗号化され安全です。また、WAN側IPアドレスを指定するため利用者が自宅からISP経由などで接続を行なっても、アクセスすることが可能です。

但し、WAN側IPアドレスにHTTPS経由でアクセスするには、「sysuser」のパスワードが必要です。※管理者メニューで設定、変更が可能です。

このパスワードの取り扱いには、十分注意して下さい
メールでの通知は避け、口頭もしくは紙、フロッピーなどで利用者にお渡し下さい
紙、フロッピーは、利用者が責任を持って保管するか
削除・廃棄することを徹底して下さい

(b) HTTP経由LAN側IPアドレスへアクセス

LAN側IPアドレスを指定するため、社内からのアクセスしか出来ません。HTTPで通信するため通信内容は保護されません。

2. PRAポートフォワードクライアントのダウンロード

ポートフォワードクライアントをダウンロードする際に、利用者は接続時のパスフレーズを設定する必要があります。このパスフレーズは、Digital Gateのユーザーメニューへアクセスするためのパスワードとは別のもので、パスフレーズに使用できる文字は、半角英数字、半角スペース、半角記号(!"#\$%&'<>?_){|~=)()です。日本語などの2バイト文字とタブは使用できません。文字数は、半角スペースを含み128文字まで設定できます。セキュリティの面からも、10文字以上で設定することをおすすめします。

3. 圧縮ファイルの解凍

ポートフォワードクライアントは、LZH形式で圧縮されていますので、ダウンロード後に解凍ツールで解凍する必要があります。必要に応じて、利用者に解凍ツールを利用したLZH形式ファイルの解凍方法を紹介してください。

PRAポートフォワードを初めて使用する利用者向けに、周知する内容を9～10ページ『[5] PRAポートフォワードクライアントセットアップにあたって』にまとめました。こちらから、同内容のwordフォーマット(LZHで圧縮)をダウンロードできますので、ご活用ください。
[PRAエンドユーザー導入書サンプル](#)

※なお、フォーマット利用に当たっては、契約者のセキュリティポリシーを考慮し、適宜変更して下さい。このフォーマットを利用することによる損害などへの責任は負いませんので、ご了承ください。

[5] PRAポートフォワードクライアント セットアップにあたって

利用者向けサンプル

1. はじめに

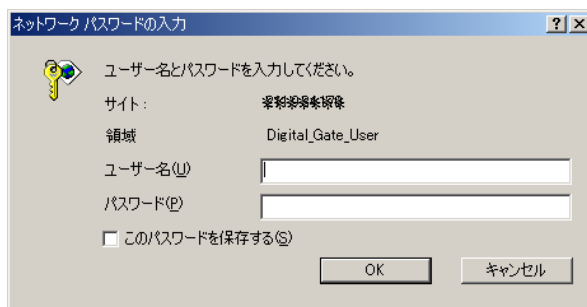
PRAポートフォワードをご利用になる場合は、このマニュアルに従って、セットアップを行なってください。セットアップ完了後は、PRAポートフォワードクライアントソフトに付属しているマニュアルをご覧ください。

2. PRAポートフォワードクライアントの入手

(a) Webブラウザから Digital Gate へアクセスする

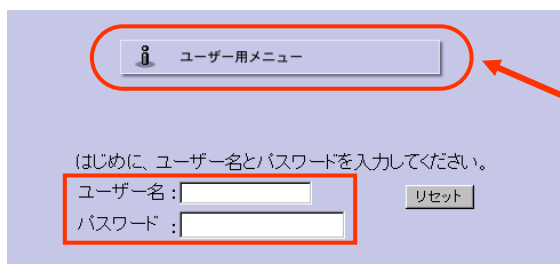
アクセスURL

(b) ブラウザのダイアログボックスが表示されるので、ユーザー名とパスワードを入力する



※ユーザー名: sysuser
パスワード: システム管理者より別途連絡

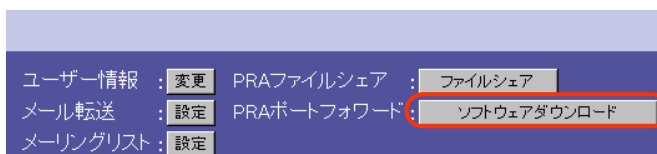
(c) ユーザー用メニューへログイン



ユーザー名とパスワードを入力し、『ユーザー用メニュー』をクリックする

※ユーザー名とパスワードが不明な場合は、システム管理者にお問い合わせください

(d) ソフトウェアダウンロードをクリックする



ソフトウェアダウンロードをクリックするとエラーになる場合はあなたがPRAポートフォワードの利用許可を受けていない可能性がありますシステム管理者にご確認をお願い致します

(e) パスフレーズを新規に設定する

PRAポートフォワードで接続する際に入力するパスフレーズを **新規に設定**して下さい。
(ユーザー用メニューのパスワードとは関係ありません)

パスフレーズに使用できる文字は、半角英数字、半角スペース、半角記号(!"#\$%&'<>?_){|~=)() です。日本語などの2バイト文字とタブは使用できません。文字数は、半角スペースを含み128文字まで設定できます。セキュリティの面からも、10文字以上で設定することをおすすめします。

パスフレーズを忘れるとPRAポートフォワードは使用出来なくなります。
忘れないように各自で管理をしてください

3. PRAポートフォワードのセットアップ

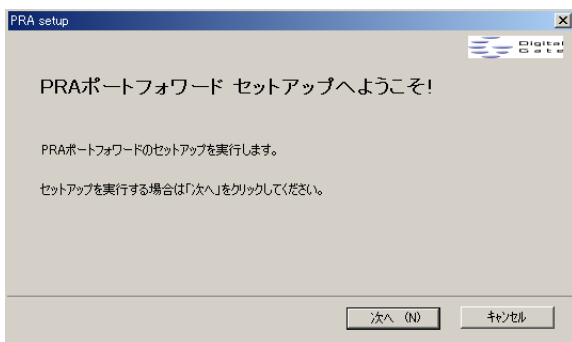
(a) ダウンロードしたファイルをPCに移動する

ダウンロードした「setup.lzh」を実際にPRAポートフォワードを使用する自宅のPCやノートPCなどに移してください。なお、このファイルは第三者の手に渡らないように、厳重に管理し、インストール後は必ず削除して下さい。

(b) setup.lzh を解凍する

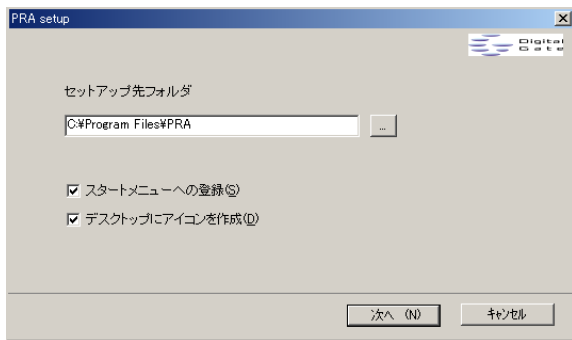
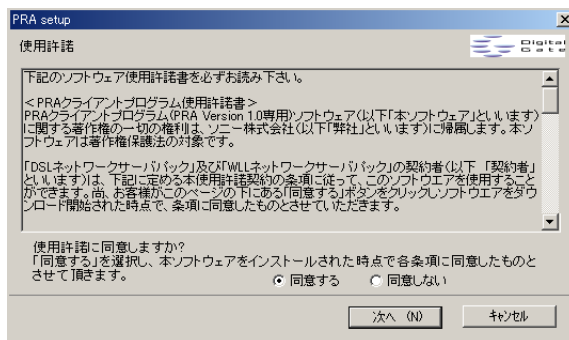
解凍ツールなどを使用して、setup.lzh を解凍して下さい。

(c) 解凍したファイルの中の『setup.exe』を実行し、セットアップを開始する



① セットアップが開始されます。『次へ』をクリックして次へ進んでください。

② 使用許諾を確認し、同意頂ける場合は「同意する」をチェックして次へ進んでください。



③ セットアップ先を指定し、続けるをクリックしてください

セットアップ完了後は必ず setup.lzh と解凍したファイルを削除してください

(d) 接続、アプリケーションの設定などは、PRAポートフォワードクライアントソフトのマニュアルを参照して下さい
インストール後のマニュアルは下記にあります。
[スタート] → [プログラム(P)] → [PRAポートフォワード] → [マニュアル]

[6] PRA転送ルール設定例

■社内のメールサーバーへアクセスする設定例①

【状況】

Digital Gateがメールサーバーである
LAN側IPアドレス:10.0.0.1

【設定方法】

PRA転送ルールを二つ投入します。

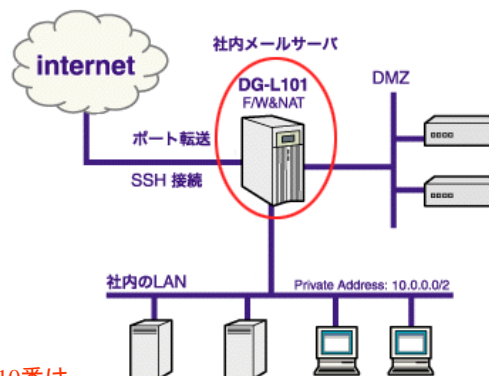
転送先IPアドレス : 10.0.0.1
転送先ポート番号 : 110
ローカルポート:10110 ←
コメント: POPサーバー

転送先IPアドレス : 10.0.0.1
転送先ポート番号 : 25
ローカルポート:25
コメント: SMTPサーバー

【ユーザーへのお知らせ】

メールソフトの設定を下記に設定して下さい。

	サーバー名	ポート番号
POPサーバー	localhost	10110
SMTPサーバー	localhost	25



ローカルポートの110番は
ウイルス駆除ソフト等で使用されている
可能性があるため違うポート番号にすることを推奨します。

■社内のメールサーバーへアクセスする設定例②

【状況】

社内LANにメールサーバーがある
メールサーバーIPアドレス:10.0.0.2

【設定方法】

PRA転送ルールを二つ投入します。

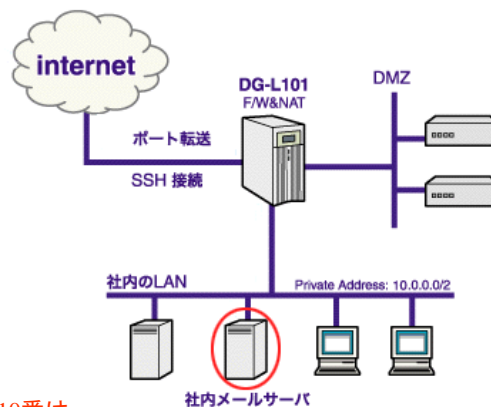
転送先IPアドレス : 10.0.0.2
転送先ポート番号 : 110
ローカルポート:10110 ←
コメント: POPサーバー

転送先IPアドレス : 10.0.0.2
転送先ポート番号 : 25
ローカルポート:25
コメント: SMTPサーバー

【ユーザーへのお知らせ】

メールソフトの設定を下記に設定して下さい。

	サーバー名	ポート番号
POPサーバー	localhost	10110
SMTPサーバー	localhost	25



ローカルポートの110番は
ウイルス駆除ソフト等で使用されている
可能性があるため違うポート番号にすることを推奨します。

■社内のWebプロキシサーバーを使用する設定例

【状況】

社内に、社内のWebにアクセスできるプロキシサーバー(Digital Gate)があり、社内のWeb全てに外部からアクセス可能としたい

LAN側IPアドレス:10.0.0.1

プロキシサーバーのポート番号:8080

【設定方法】

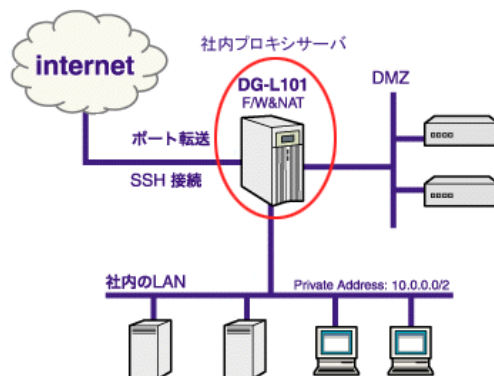
下記のPRA転送ルールを設定します。

転送先IPアドレス : 10.0.0.1
 転送先ポート番号 : 8080
 ローカルポート:8080
 コメント: プロキシサーバー

【ユーザーへのお知らせ】

Webブラウザのプロキシを下記に設定することで社内のWebが閲覧できます。

プロキシサーバー名	ポート番号
localhost	8080



■社内のWebサーバーを閲覧する設定例

【状況】

社内に複数のWebサーバーがあるが、そのうち2つのサーバーのみ外部からアクセス可能にしたい

Webサーバー①IPアドレス:10.0.0.3

Webサーバー②IPアドレス:10.0.0.4

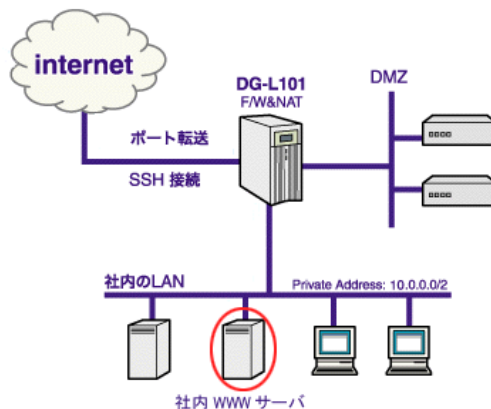
【設定方法】

下記のPRA転送ルールを設定します。

転送先IPアドレス : 10.0.0.3
 転送先ポート番号 : 80
 ローカルポート:4080 ←
 コメント: Webサーバー①

転送先IPアドレス : 10.0.0.4
 転送先ポート番号 : 80
 ローカルポート:5080 ←
 コメント: Webサーバー②

複数のWebサーバーを設定する場合は、ローカルポートが重複しないように設定して下さい。



【ユーザーへのお知らせ】

Webブラウザで下記のURLにアクセスして下さい。

Webサーバー① http://localhost:4080/
 Webサーバー② http://localhost:5080/